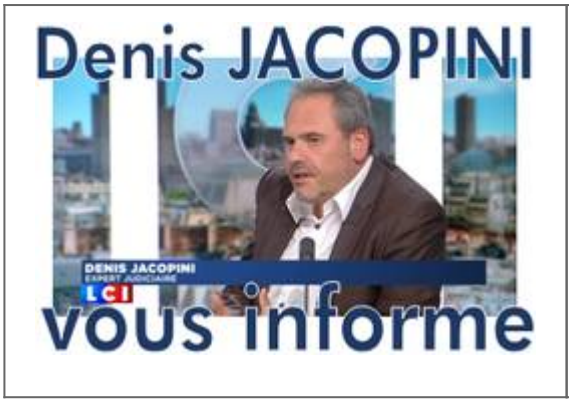
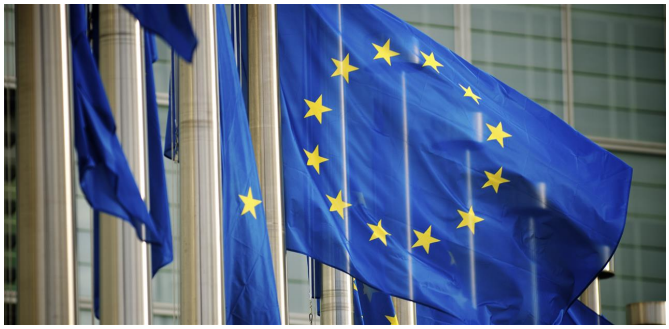
Directive sur la cybersécurité : Amazon, eBay, Google devront notifier leurs incidents majeurs – Next INpact



Directive sur la cybersécurité : Amazon, eBay, Google devront notifier leurs incidents majeurs

Après des heures de négociations, le Parlement européen et les États membres sont arrivés lundi à un accord sur la future directive NIS (network and information security). Un texte destiné à mieux protéger les opérateurs dits critiques dans toute l'Europe.



Cette future directive sur la cybersécurité visera en effet à imposer des règles harmonisées à tout un ensemble d'opérateurs critiques. Le mouvement sera épaulé par le réseau des Computer Security Incident Response Team (CSIRT) pour discuter des incidents et identifier de possibles réponses coordonnées.

Plusieurs niveaux de reporting selon les acteurs concernés

Ce texte visera avant tout à définir des critères pour savoir qui relève de ces obligations. En tête de liste, on trouvera nécessairement les acteurs de l'énergie, du transport et de la santé. Selon l'eurodéputé Andreas Schwab (EPP), ces entreprises devront répondre à plusieurs mesures de sécurité, mais également notifier aux autorités les incidents de cybersécurité qualifiés « *d'importants.* »

Si les micro entreprises et les PME seront épargnées, les principaux acteurs du Net seront également concernés, mais avec des obligations finalement plus en retrait. Sont cités les marketplaces comme Amazon ou eBay, les moteurs de recherche mais aussi les services de cloud qui devront mettre en place de mesures de sécurité tout en rapportant aux autorités les seuls « *incidents majeurs* » qui viendraient les impacter.

Le flou règne par contre sur les autres plateformes en ligne comme les réseaux sociaux. Selon l'eurodéputé, toutefois, « *cette directive marque le début de la régulation des plateformes. Alors que la consultation de la Commission européenne sur ces acteurs est toujours en cours, les nouvelles règles prévoient déjà des définitions concrètes – une demande du Parlement européen exprimée depuis le début des négociations –*, afin de faire connaître son consentement à l'inclusion des services numériques. »

En aout dernier, l'obligation de reporter aux autorités les incidents de sécurité avait soulevé les inquiétudes des représentants du secteur. Selon l'Afdel, l'association française des éditeurs de logiciels et de solutions Internet, une obligation indifférenciée de reporting « *pourrait porter atteinte à la compétitivité des entreprises du numérique, en particulier des entreprises françaises et européennes du numérique – dont de nombreuses PME, qui n'ont pas toute la capacité d'adaptation des grands groupes internationaux –, sans atteindre les objectifs poursuivis en termes de sécurité* ». L'ASIC, l'association des services Internet communautaires, avait craint pour sa part de voir chaque État membre devenir « *le Directeur des services informatiques de l'ensemble des acteurs du numérique* », du moins si des critères trop larges étaient inscrits en dur dans le texte final.

Le projet de directive doit maintenant être approuvé formellement par la Commission au marché intérieur du Parlement européen et par le Comité des représentants permanents.

Des obligations de reporting préexistent dans certains secteurs et en France

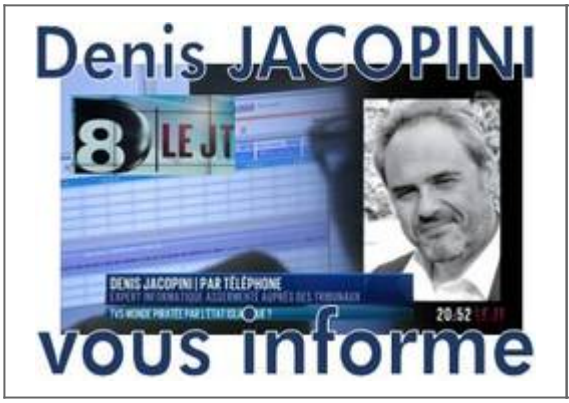
Suite à l'adoption du Paquet Télécom en Europe, rappelons que les opérateurs télécom doivent déjà notifier les fuites de données personnelles aux autorités de contrôle des données personnelles (la CNIL, ici). En France, l'Agence nationale de la sécurité des systèmes d'information chapeaute pour le compte du premier ministre, les règles de sécurité que doivent suivre les OIV, ces opérateurs d'importance vitale dont l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.

Depuis la loi de programmation militaire de 2013, centrales nucléaires, hôpitaux, sociétés de transports, acteurs des télécoms, etc. ont l'obligation de fournir « *les informations nécessaires pour évaluer la sécurité de ses systèmes d'information, notamment la documentation technique des équipements et des logiciels utilisés dans ses systèmes ainsi que les codes sources de ces logiciels.* »

Réagissez à cet article

Source : http://www.nextinpact.com/news/97630-directive-sur-cybersecurite-amazon-ebay-google-devront-notifier-leurs-incidents-majeurs.htm

La CNIL demande à Facebook de ne pas tracer les non-membres



La CNIL demande à Facebook de ne pas tracer les non-membres

À la suite du jugement belge exigeant de Facebook qu'il mette fin au pistage des internautes, cinq autorités de protection de la vie privée demandent au réseau social d'appliquer les conséquences du verdict sur l'ensemble de l'Union européenne.

Dans son bras de fer contre Facebook, qui est accusé de suivre tous les internautes à la trace, y compris ceux qui ne sont pas inscrits sur le réseau social, la commission de la protection de la vie privée belge n'est pas seule. L'institution peut en effet compter sur le soutien de quatre autres autorités européennes.

Celles-ci ont en effet publié une déclaration commune qui réclame la fin de l'ingérence du site américain dans la vie privée des internautes. Ce texte fait suite au jugement rendu en première instance par le tribunal civil de Bruxelles, qui condamne Facebook à cesser de tracer l'activité des internautes en Belgique lorsqu'ils visitent des sites web sur lesquels sont installés des boutons de partage, comme le célèbre « J'aime ».

Les autorités de France, de Belgique, d'Espagne, des Pays-Bas et de Hambourg sur la même ligne.

« Tout en reconnaissant le droit de Facebook à faire appel de ce jugement, le Groupe de contact attend de la société qu'elle se conforme à ce jugement sur tout le territoire de l'Union européenne », écrivent-elles. Elles ajoutent, dans un communiqué, que cette immixtion « n'est pas acceptable » et que Facebook doit « prendre les mesures nécessaires pour se mettre en conformité » avec les règles communautaires.

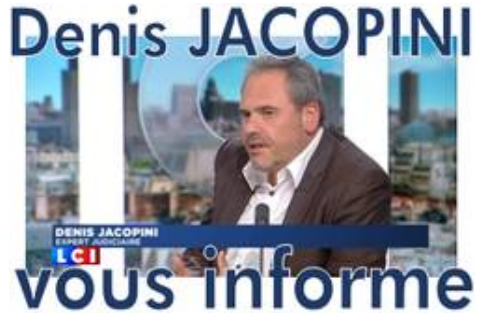
Mais en la matière, les mesures que Facebook a déjà déployées pour respecter le jugement de la justice belge ont eu pour effet d'irriter la commission de la protection de la vie privée belge. En effet, au lieu de neutraliser le cookie litigieux (intitulé « datr » et que Facebook justifie au nom de la sécurité de ses membres), le réseau social a préféré bloquer l'accès aux internautes belges qui ne sont pas connectés au service.

Réagissez à cet article

Source : http://www.numerama.com/politique/133980-la-cnil-demande-a-facebook-de-ne-pas-tracer-les-non-membres.html

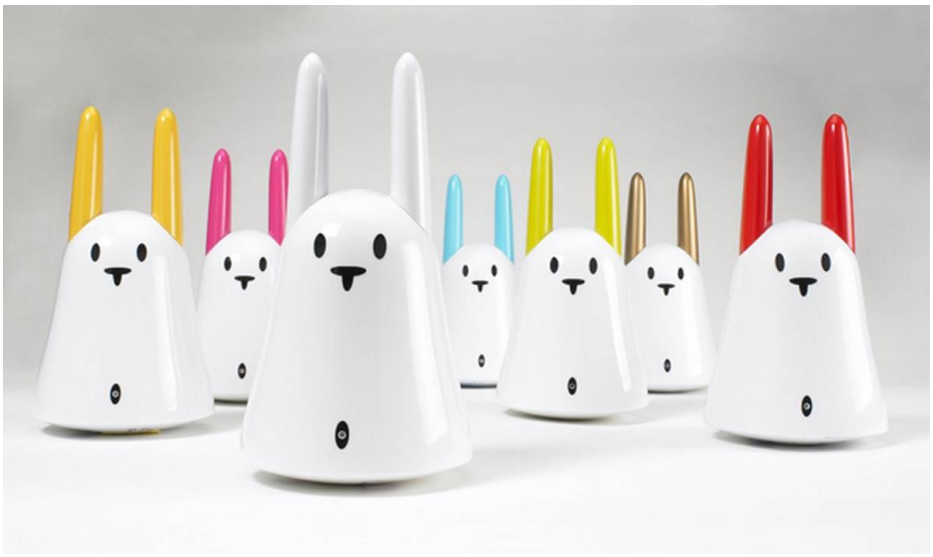
---

Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ?



Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ?

Télévision, pèse-personne, thermostat et autres hubs domotiques… les objets connectés tentent d'envahir nos maisons et de s'infiltrer au coeur même de leur réseau numérique.



Pourtant, malgré leur objectif de nous simplifier la vie, leur développement semble encore assez poussif ; en raison sans doute de leur manque criant de sécurité. C'est ce que révèle une étude menée par la division Sécurité de Hewlett Packard : rien de moins que 250 vulnérabilités ont été relevées par les experts d'HP Fortify au sein des 10 objets connectés les plus populaires.

Ces failles de sécurité seraient, selon Mike Amistead, le manager général d'HP Fortify, le symptome de la ruée des entreprises sur le créneau des objets connectés. Il estime en effet que les start-ups se lançant sur ce marché tenteraient de commercialiser leur produit le plus rapidement possible avant la concurrence… au mépris de la garantie d'un niveau de sécurité suffisant des réseaux et des données personnelles.

Vos données personnelles en clair sur la toile

Parmi les failles de sécurité relevées, HP a constaté que :

– 90 % des objets connectés étudiés solliciteraient une information personnelle sensible (ex : adresse email ou postale, nom, date de naissance, etc) ; une information ensuite véhiculée en clair sur la toile ;

– 70 % des objets connectés ne crypteraient pas les données échangées avec le réseau ;

– 80 % des objets connectés ne nécessiteraient pas de mot de passe complexe pour identifier les demandes de connexion tierces ;

– 60 % des objets connectés seraient vulnérables aux attaques dites de « cross-site scripting » (type de faille de sécurité permettant d'injecter du contenu dans une page, et provoquant ainsi des actions sur les navigateurs web visitant la page).

Réagissez à cet article

Source : http://www.archimag.com/vie-numerique/2014/07/30/objets-connectes-internet-failles-securite

Le Conseil de l’UE rend sa copie sur la directive cybersécurité

	Le Conseil de l’UE rend sa copie sur la directive cybersécurité

Les députés et le Conseil des ministres de l'UE sont parvenus à un accord autour de la directive NIS (Network and Information Security.) Celle-ci entend harmoniser les exigences en matière de cybersécurité entre les 28 pays membres de l'UE.

L'Europe ouvre la voie à une gestion communautaire de la cybersécurité et annonce un accord entre le parlement et le Conseil de l'UE autour de la directive NIS.

Cette directive en négociation depuis plusieurs mois est chargée d'harmoniser le cadre légal des pays membres autour des dispositions relatives à la sécurité des systèmes jugés critiques. La directive était en discussion au conseil depuis le mois d'octobre 2014, après une validation du parlement et à l'époque, les négociations s'annonçaient serrées.

Le texte initial s'accordait sur la nécessité pour les opérateurs « critiques » de faire remonter auprès des responsables et autorités les incidents de sécurité qui pouvaient affecter leurs systèmes. Derrière ce terme, on retrouvait ceux qu'en France on place sous la catégorisation d'OIV (opérateurs d'importance vitale) depuis la loi de programmation militaire de 2013 : les acteurs majeurs du secteur de l'énergie, des transports, de la santé ou des marchés financiers par exemple.

Mais le texte revu et corrigé par le Conseil de l'UE va plus loin et propose d'étendre la régulation des plateformes en ligne à l'instar de Google, Amazon ou Ebay. Ces plateformes en ligne devront donc également se plier à des exigences de reporting en matière de cybersécurité, mais celles-ci seront moins lourdes que les exigences envisagées pour les opérateurs critiques. Seuls les incidents graves devront être signalés.

Les États membres auront pour rôle d'identifier les acteurs et plateformes jugés « indispensables pour la société et l'économie » en amont, mais le texte prend soin d'exclure les micro et petites entreprises du numérique, qui jouiront d'une exemption.

Mieux vaut prévenir que subir

Le texte prévoit également la création d'un « réseau d'équipes d'intervention en cas d'incident lié à la sécurité informatique » établi dans chaque état membre afin de traiter et de répondre aux incidents transfrontaliers et « identifier des réponses coordonnées.

Reuters avait déjà publié en août un article relatant l'évolution des négociations en ce sens, une information qui avait suscité les inquiétudes de l'Afdel et de l'Asic. Les associations d'éditeurs en ligne craignaient en effet une loi trop pesante venant désavantager les entreprises et plateformes web européennes face à leurs concurrents étrangers.

Le texte doit encore être approuvé par la commission du marché intérieur du Parlement et par le comité des représentants permanents du Conseil avant d'être appliqué. En l'état actuel du texte, force est de reconnaître que cela ne devrait pas changer fondamentalement la donne en France : le reporting des incidents affectant les OIV était déjà l'une des mesures phares de la loi de Programmation Militaire de 2013 tandis que l'Anssi assume de fait le rôle d'équipe d'intervention en cas d'incident.

Mais la mention des plateformes web parmi les acteurs concernés pourrait en revanche amener le gouvernement à élargir la liste des OIV à placer sous la coupe de la LPM afin de se mettre en harmonie avec la directive européenne.

Réagissez à cet article

Source : http://www.zdnet.fr/actualites/le-conseil-de-l-ue-rend-sa-copie-sur-la-directive-cybersecurite-39829484.htm

---

Le FBI et Microsoft font

trembler le botnet DorkboOscar Barthe

Le FBI et Microsoft font trembler le botnet Dorkbot

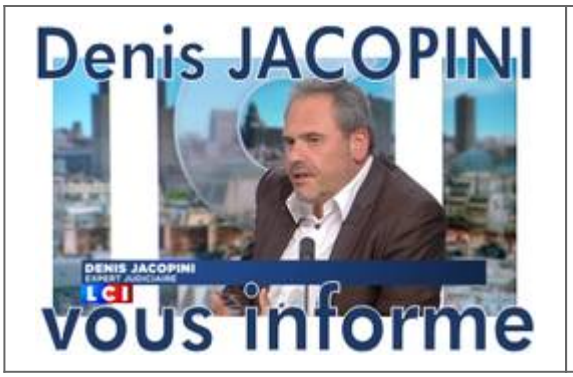
En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.

Le botnet Dorkbot permet à ses utilisateurs de récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Twitter ou encore Steam.
En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.
Microsoft a fait sa bonne action. La firme de Redmond a déclaré jeudi avoir collaboré avec les autorités de plusieurs régions pour perturber le fonctionnement du botnet Dorkbot.
Découvert il y a quatre ans, ce dernier a infecté aujourd'hui plus d'un millions de machine. Il est utilisée pour récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Netflix, PayPal, Steam ou encore eBay. La firme de Redmond ne s'est toutefois pas lancée seule dans l'attaque contre Dorkbot, et a travaillé ainsi avec le fournisseur de solution de sécurité Eset, le Cert polonais Polska, la commission canadienne de Radio-télévision et de télécommunications, l'agence de sûreté américaine, le FBI, Interpol, Europol et la police montée du Canada.
Les utilisateurs sont pour la majeure partie d'entre eux infectés lors de leur navigation sur internet sur des sites pas forcément bien protégés. Dorkbot exploite la moindre faille logicielle via un exploit kit ou les spam. Il peut aussi utiliser un système de ver pour se diffuser à travers les réseaux sociaux, les services de messagerie ou les clés USB.

Une attaque efficace mais pas durable
Microsoft n'a toutefois pas détaillé comment il s'y était pris pour perturber les infrastructures de Dorkbot. Ce n'est d'ailleurs pas la première fois que la firme collabore avec les autorités dans ce genre de situation. Les actions coordonnées visant à déconnecter les serveurs hébergeant les botnet ont souvent un impact immédiat mais les bénéfices ne durent pas. Souvent, les cybercriminels remettent rapidement sur pied une nouvelle infrastructure et s'attaque à la reconstruction du botnet en infectant d'autres ordinateurs.
La situation autour de Dorkbot devenait critique. Ses créateurs ont diffusé un kit permettant d'utiliser le botnet comme base pour en construire d'autres, plus puissants. Baptisé NgrBot, il était en vente sur le deep web.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-le-fbi-et-microsoft-font-trembler-le-botnet-dorkbot-63185.html
Par Oscar Barthe

Les CNIL européennes haussent le ton contre le pistage de Facebook



Les CNIL européennes haussent le ton contre le pistage de Facebook

Après une décision de la justice belge, d'autres pays européens réclament que Facebook cesse de traquer les internautes en dehors de ses pages.

Facebook n'est pas encore sorti du bourbier européen.

L'autorité française de protection des données (la CNIL) a publié lundi une déclaration commune avec quatre de ses homologues européens concernant les règles de confidentialité du réseau social.

Elle fait suite à une décision de la justice belge, qui a demandé à Facebook de ne plus tracer les internautes non-inscrits sur le site américain. L'entreprise a finalement obtempéré il y a une semaine, en empêchant toute personne sur le territoire belge déconnectée du site d'accéder à ses pages.

Pas encore suffisant pour les cinq CNIL des Pays-Bas, de la France, de l'Espagne, de Hambourg et de la Belgique, qui réclament la généralisation du dispositif. «Le groupe de contact attend de la société qu'elle se conforme à ce jugement sur tout le territoire de l'Union européenne», précise le communiqué.

Mesures de sécurité

En Belgique, la justice contestait l'utilisation par Facebook d'un «cookie», un micro-fichier qui conserve les données ou habitudes des internautes, baptisé «datr».

Principale critique: cette collecte concerne les personnes ne disposant pas de compte Facebook, et qui ne consentent donc pas à ce suivi. Il suffit de visiter une page du site (par exemple un évènement public) pour se voir déposer ce cookie sur son ordinateur et mobile. Facebook est ensuite capable de connaître les fréquentations en ligne de l'internaute, s'il se rend sur des sites contenant des modules du réseau social, comme le bouton «like».

De son côté, Facebook affirme qu'il collecte des cookies pour des raisons de sécurité. «Nous les utilisons afin de distinguer les véritables visites des fausses», expliquait la semaine dernière Alex Stamos, en charge de la sécurité chez Facebook. «Depuis cinq ans, ces cookies nous servent à empêcher la création de faux comptes, d'empêcher le vol de données ou l'organisation d'attaques par déni de service.» Facebook précise que ces cookies sont utilisés afin de surveiller le comportement d'un navigateur Web, et non d'un utilisateur précis. Pour Alex Stamos, «si le cookie nous informe qu'un navigateur a visité des centaines de sites en cinq minutes, cela nous indique qu'il s'agit probablement d'un robot».

Facebook a ajouté qu'il comptait faire appel de la décision de la justice belge et qu'il était prêt à discuter du sujet du cookie «datr» avec les autres autorités de protection des données.

Le groupe des CNIL européennes dénonce lui une «ingérence dans la vie privée des internautes» qui «n'est pas acceptable». Il réclame à Facebook de «prendre les mesures nécessaires pour se mettre en conformité avec la législation européenne, et ce sur tout le territoire de l'Union européenne.»

Le groupe enquête depuis presque un an sur les règles de confidentialité de Facebook. Ces investigations sont menées par chacune des CNIL, mais coordonnées par le groupe de contact. Leurs conclusions ne devraient pas être rendues avant l'année prochaine.

Réagissez à cet article

Source : http://www.lefigaro.fr/secteur/high-tech/2015/12/07/32001-20151207ARTFIG00299-les-cnil-europeennes-haussent-le-ton-contre-le-pistage-de-facebook.php

Safe Harbor et localisation des données

Safe Harbor et localisation des données

Après l'invalidation du Safe Harbor, Max Shrems pousse son avantage, et veut obliger les CNIL européennes à tirer les conséquences de la fin de cet accord. Et à obliger les GAFA à stocker les données personnelles des Européens sur le continent.

Un jeune Autrichien en 28 ans va-t-il faire plus pour la régulation du Cloud sur le Vieux Continent que la Commission Européenne depuis dix ans ?
L'activiste Maximilian Schrems, (en photo) déjà à l'origine de l'invalidation de l'accord dit Safe Harbor par la Cour de justice européenne (CJUE), ouvre un nouveau front, touchant cette fois à la localisation des données personnelles des citoyens européens.

Sa cible, une fois encore : Facebook.

Schrems demande cette fois à plusieurs CNIL en Europe d'ordonner au réseau social de conserver ses données sur le sol européen, arguant du fait qu'il n'existe plus (et pour cause) de cadre légal assurant le transfert de ses données sur le sol américain en toute sécurité. Pour ce faire, l'activiste a déposé deux nouvelles plaintes contre Facebook. La première auprès de l'autorité belge de protection des données, la seconde auprès de l'équivalent de la CNIL en Allemagne.
Max Schrems a également mis à jour sa plainte auprès de l'autorité irlandaise, celle qui avait abouti à l'invalidation du Safe Harbor. Rappelons que Facebook opère ses activités hors des Etats-Unis depuis l'Irlande, raison pour laquelle Schrems avait choisi ce pays pour s'attaquer au réseau social. L'autorité irlandaise s'étant déclaré incompétente, la plainte avait été transmise à la CJUE qui avait fini par invalider le Safe Harbor, accord de 2001 autorisant les entreprises établies aux États-Unis, notamment les GAFA (Google, Apple, Facebook, Amazon), à recevoir des données en provenance de l'Union européenne dans un cadre légal. La CJUE a décidé de tirer un trait sur cet accord à la lumière des révélations d'Edward Snowden sur les programmes de surveillance de la NSA et sur la complicité des grands noms du Web – dont Facebook – à ces programmes.

Forcer la main des CNIL européennes

Cet accord n'existant plus, Max Schrems estime que les transferts de données vers les Etats-Unis violent la loi européenne, qui réclame que ces exports ne peuvent être effectués vers un pays offrant un niveau de protection inférieur à celui de la loi en place sur le Vieux Continent. Le jeune Autrichien se demande donc sur quelles bases légales sont assurés les transferts de ces données vers les États-Unis. Interpelé sur ce point le 12 octobre (quelques jours après la décision de la CJUE), Facebook a produit tardivement un accord contractuel, daté du 20 novembre 2015, passé entre sa filiale irlandaise et sa maison mère et encadrant les transferts d'informations entre les deux entités. « En plus de cet accord, Facebook Ireland se base sur un certain nombre d'autres moyens légaux pour transférer les données de ses utilisateurs aux Etats-Unis », assurent les avocats du réseau social, dans une lettre. Sans plus de précisions toutefois. Max Schrems conteste la légalité de ces accords, censés suppléer la disparition du Safe Harbor, au regard des révélations d'Edward Snowden sur des programmes de surveillance comme Prism.

Pour forcer les CNIL européennes à prendre ce qu'il estime être tirer les conséquences logiques de la décision de la CJUE, le jeune Autrichien pourra s'appuyer sur les fractures qui apparaissent entre ces différentes autorités de contrôle. Fin octobre, l'administration allemande a mis en doute la voie préconisée par la Commission européenne après la fin du Safe Harbor, soit la mise en place rapide d'alternatives basées sur des accords contractuels. Indiquant qu'elle bloquerait tout nouveau transfert de données exploitant ces mécanismes.
Conséquence, selon Johannes Caspar, le responsable allemand de la protection des données : « Quiconque souhaite échapper aux conséquences légales et politiques du jugement de la CJUE devrait dans le futur étudier le stockage des données personnelles uniquement sur des serveurs situés au sein de l'UE ».
Max Schrems explique que les plaintes déposés en Irlande, en Belgique et en Allemagne font partie d'un « premier round » ; d'autres devraient suivre dans d'autres juridictions européennes.
Dans un communiqué, l'activiste précise : « je n'ai aucune doute qu'une large majorité des autorités européennes de protection des données enquêteront correctement sur les plaintes et prendront les actions qui s'imposent. Néanmoins, dans un cas particulier, j'ai senti le besoin de clarifier le fait qu'une résistance délibérée à faire le travail pourrait avoir des conséquences personnelles pour les responsables concernés ».

Safe Harbor 2 dans l'urgence

Rappelons que, suite à l'invalidation du Safe Harbor, la Commission européenne a relancé dans l'urgence des négociations pour aboutir rapidement à un nouvel accord cadre. Ce Safe Harbor 2 devra répondre pleinement aux exigences de la CJUE, pour que le cadre résiste aux défis juridiques posés par les régulateurs en charge de la protection des données.
Réunis au sein du groupe des CNIL européennes (G29), ces derniers attendent des autorités européennes et américaines une solution « satisfaisante » avant le 31 janvier 2016. Nul doute que Max Schrems n'est de toute façon pas disposé à leur laisser davantage de temps.

Réagissez à cet article
Source : http://www.silicon.fr/max-schrems-le-tombeur-du-safe-harbor-sattaque-a-la-localisation-des-donnees-133129.html

---

Objets connectés : les Français sont séduits mais restent méfiants

Objets connectés : les Français sont séduits mais restent méfiants

L'internet des objets, terrain de jeu de nombreuses start-up et d'entreprises industrielles, entre doucement dans les habitudes de consommation des Français.

Réalisé par le Credoc pour le compte du Conseil général de l'économie (CGE) et de l'Autorité de régulation des communications électroniques et des postes (Arcep), le baromètre du numérique 2015 vient de paraître.
Cette enquête, destinée à faire le point sur la diffusion des technologies de l'information dans la société française, s'est notamment portée sur l'accueil réservé par les consommateurs aux objets connectés.
Il en ressort que 6 % des Français utilisent déjà des outils leur permettant de commander à distance des appareils électroniques présents à leur domicile. Un chiffre qui reste modeste et qui n'a augmenté que de deux points depuis la dernière étude réalisée en 2011.
Sans surprise, les jeunes adultes (8 %), les plus diplômés (8 %), les cadres supérieurs (13 %) et les habitants de la région parisienne (10 %) sont les plus friands de ces solutions domotiques. Quant à leur adoption prochaine, 33 % des Français déclarent l'envisager (contre 25 % en 2011). Les 12 à 17 ans (60 %), les hauts revenus (40 %) et les habitants de la région parisienne (40 %) sont sur ce point les plus catégoriques.

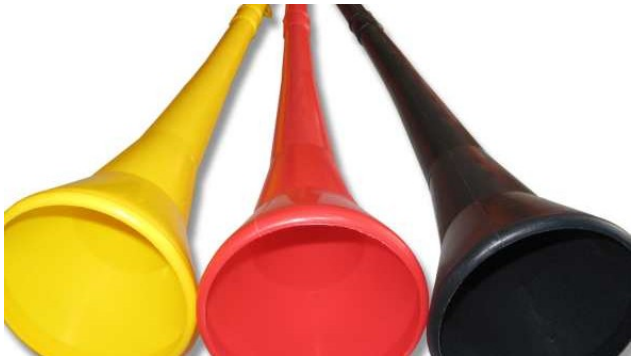
Un frein sur les objets connectés « santé »
La santé est un des principaux axes de développement de l'Internet des objets. Interrogés sur ces solutions, les Français les considèrent comme intéressantes lorsqu'elles sont destinées à recueillir des données permettant d'améliorer leur état de santé (28 %), à mieux gérer leur poids (24 %) ou bien leur sommeil (21 %).
En revanche, ils font preuve, à une écrasante majorité, d'une réelle défiance vis-à-vis des entreprises qui fabriquent et commercialisent ces objets connectés. 83 % estiment ainsi qu'elles feront un usage commercial des informations recueillies sur leur santé. Une opinion très ancrée chez les cadres supérieurs (92 %) et les plus diplômés (91 %). En outre, 78 % considèrent que ces entreprises sont incapables de garantir une parfaite protection de ces données personnelles et privées.

Réagissez à cet article
Source : http://business.lesechos.fr/entrepreneurs/web/7000261-objets-connectes-les-francais-sont-seduits-mais-restent-mefiants-205224.php

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela, une messagerie qui cache les métadonnées

Vuvuzela est une nouvelle messagerie qui prétend qu'elle peut cacher les métadonnées. Le concept est encore très expérimental, mais il est assez prometteur.

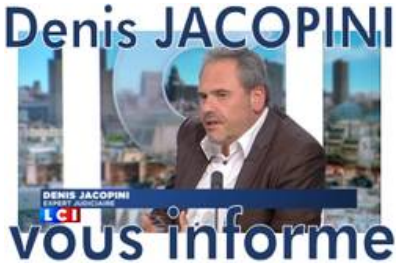


Vuvuzela est un concept de messagerie qui permet de communiquer en cachant les métadonnées. Elle est développé par David Lazar, un doctorant du MIT qui travaille sur le chiffrement et les systèmes distribués. Il a publié un papier qui décrit les principes de Vuvuzela.
Des protocoles comme TOR permettent d'avoir un certain anonymat, mais il reste vulnérable à une analyse du trafic. Avec Vuvuzela, la messagerie est spécialement conçue pour se protéger contre la surveillance gouvernementale sur les métadonnées. La NSA a admis a plusieurs reprises qu'il ne sert à rien de chiffrer les données si les métadonnées sont en clair.

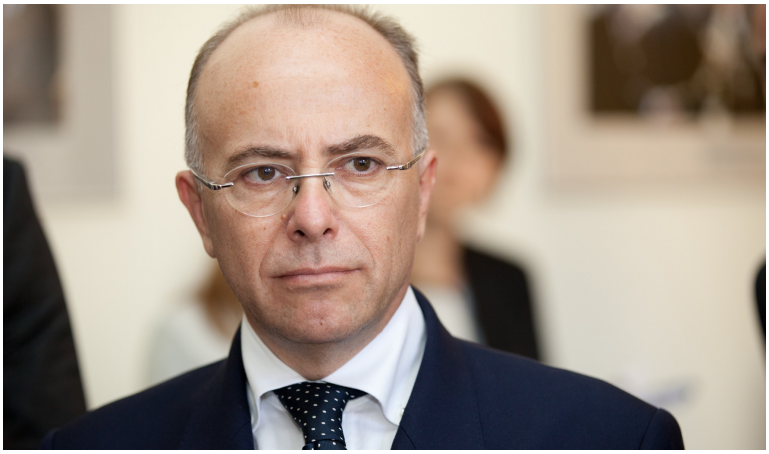
Les métadonnées englobe de nombreuses informations, mais on peut les résumer par le fait qu'elle pointent vers l'identité d'une personne et les contacts de cette personne. Vuvuzela veut cacher les métadonnées, mais elle ne peut pas cacher 2 métadonnées. La première est le nombre d'utilisateurs connectés sans une conversation et la seconde concerne les utilisateurs actifs dans une conversation. Mais Vuvuzela réduit également ce problème en ajoutant des nuisances aux métadonnées.
Le concept est intéressant, mais il n'est pas prêt pour le déploiement. On peut suivre le projet sur Github.

Réagissez à cet article
Source : http://actualite.housseniawriting.com/technologie/2015/12/04/vuvuzela-une-messagerie-qui-cache-les-metadonnees/11327/

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement



Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement



La liste des mesures envisagées par le gouvernement pour renforcer la sécurité au détriment de la liberté et de la vie privée s'allonge. Alors que le gouvernement envisage déjà de nouvelles lois sécuritaires qui permettraient par exemple de croiser tous les fichiers de données personnelles détenues par l'État, d'obliger à l'installation d'émetteurs GPS sur les voitures louées, d'allonger la durée de conservation des données de connexion ou encore de faciliter le recours aux IMSI-catchers, Le Monde révèle samedi de nouvelles mesures recensées par le ministère de l'Intérieur.
Le quotidien a en effet pu consulter un tableau édité en interne le mardi 1er décembre par la direction des libertés publiques et des affaires juridiques (DLPAJ), qui dépend du ministère de l'Intérieur de Bernard Cazeneuve. C'est elle qui prépare les projets de lois et de décrets relatifs aux libertés publiques et à la police administrative. C'est donc dans ce cadre, pour rédiger deux nouveaux textes législatifs – l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme, que la DLPAG a dressé les mesures demandées par la police ou la gendarmerie qui pourraient être inscrites dans les textes attendus pour janvier 2016.

Interdire et bloquer TOR en France
Parmi ces mesures qui ne sont encore que des hypothèses de travail figure une série de nouvelles restrictions aux libertés sur Internet :
« Interdire les connexions Wi-Fi libres et partagées » et fermer toutes les connexions Wi-Fi publiques pendant l'état d'urgence, « sous peine de sanctions pénales ».
Jusqu'à présent la loi impose par principe aux abonnés à internet de sécuriser leur connexion pour éviter qu'elle soit utilisée à des fins illicites, mais le seul risque que prennent les abonnés généreux et récalcitrants qui laissent leur Wi-Fi ouvert est de recevoir un avertissement Hadopi si quelqu'un l'utilise pour pirater des films ou de la musique. En obligeant à fermer toute connexion, la police s'assurerait d'avoir un identifiant précis pour chaque adresse IP, ou au moins de réduire la liste des suspects possibles dans un même foyer. C'est en tout cas l'idée.
« Interdire et bloquer les communications des réseaux TOR en France » : Même à supposer que ça soit techniquement possible, ce serait une mesure totalement disproportionnée qui enverrait un très mauvais signe à l'international, alors que le réseau d'anonymisation TOR est utilisé par de très nombreux activistes et dissidents de pays autoritaires. L'un des premiers pays à avoir bloqué Tor était l'Iran.
« Identifier les applications de VoIP et obliger les éditeurs à communiquer aux forces de sécurité les clefs de chiffrement » : C'est la fameuse grande guerre du chiffrement à laquelle se prépare La Quadrature du Net, la France ayant sans aucun doute la volonté de se joindre à la Grande-Bretagne pour obtenir que les éditeurs de messagerie chiffrée fournissent des backdoors pour que les autorités puissent écouter les conversations interceptées.

Réagissez à cet article
Source : http://www.numerama.com/politique/133795-wi-fi-ouvert-interdit-tor-bloque-les-nouvelles-idees-de-la-police.html